Amendments to the Specification

Please replace the paragraph that begins on Page 1, line 4 and carries over to Page 2, line 4 with the following marked-up replacement paragraph:

– The present invention is related to the following commonly-assigned U. S. Patents, all of which were filed on 12/05/2001 and which are hereby incorporated herein by reference: U. S. Patent _____ (serial number 10/007,593), entitled "Kernel-Based Security Implementation"; U. S. Patent _____ (serial number 10/007,446), entitled "Policy-Driven Kernel-Based Security Implementation"; U. S. Patent _____ (serial number 10/007,582), entitled "Offload Processing for Secure Data Transfer"; and U. S. Patent _____ (serial number 10/007,581), entitled "Offload Processing for Security Session Establishment and Control". These U. S. Patents are referred to hereinafter as "the related inventions". The present invention is also related to commonly-assigned U. S. Patent _____ (serial ~~number 10/_____), entitled~~ number 10/058,870), entitled "Integrated Intrusion Detection Services", which was filed concurrently herewith. –

Please replace the paragraph that begins on Page 8, line 18 and carries over to Page 9, line 7 with the following marked-up replacement paragraph:

– The technique may further comprise: specifying, for each of a plurality of potential intrusion events, a set of one or more conditions which describe the potential intrusion event; associating a ~~sensitivity~~ suspicion level with each of the sets of conditions; and determining a suspicion level of the particular inbound communication. In this case, using the defined intrusion suspicion levels preferably determines that the particular inbound communication should be

treated as an intrusion event when conditions pertaining to the particular inbound communication match a selected one of the sets of conditions and the determined suspicion level maps to the ~~sensitivity~~ suspicion level associated with the selected set of conditions. --

Please replace the paragraph on Page 16, lines 1 - 9 with the following marked-up replacement paragraph:

-- The IDS policy information [[320]] 330 is preferably stored in a repository such as a network-accessible directory. For purposes of illustration but not of limitation, the repository is referred to herein as an "LDAP directory". (LDAP directories are well known in the art, and will not be described in detail herein.) Use of a network-accessible directory promotes uniform treatment of intrusion detection throughout an enterprise, as the administrator can work with consistent policy formats for all intrusion detection sensors. Preferably, an object-oriented directory or database is used, in order to take advantages of relationships among data to narrow the search process as well as to efficiently associate response data with broad classes of attacks. ("Classes" of attacks will be described in more detail below.) --

Please replace the paragraph on Page 28, lines 10 - 16 with the following marked-up replacement paragraph:

-- Optionally, signature files may be organized or partitioned to provide more efficient processing. When the comparison against attack signatures is to be performed within error-handling logic, according to the optimization disclosed herein, contextual information is known that may limit the potential candidate signatures. Thus, only those signatures which are pertinent

to this context need to be compared to the suspected attacking packet. For example, signatures pertaining to malformed packets may be grouped together, and [[using]] used in error-handling logic that is invoked when a malformed packet is detected. --